2. (original) The method of encoding transaction data of claim 1, wherein: said first encryption operation uses an asymmetrical encryption process; and said second encryption operation uses a symmetrical encryption process.

3. (original) The method of encoding transaction data of claim 2, wherein said symmetrical encryption process uses a secret encryption key and wherein said method includes the further step of performing a third encryption operation on said secret encryption key.

4. (original) The method of encoding transaction data of claim 1, wherein said second encryption process is performed on both the PIN and non-PIN data, such that the encrypted PIN data resides within an encrypted envelope generated by the second encryption operation.

a2

5. (original) The method of encoding transaction data of claim 1, further comprising the steps of:

calculating a digest by applying a one-way mathematical process to the non-PIN data; and

appending the digest to the PIN data blocks for future verification of the non-PIN data.

6. (currently amended) A method for decoding encrypted transaction data, the transaction data including account PIN data input by a user as well as non-PIN data, comprising the steps:

performing a first decryption operation to decode the non-PIN data; and

performing a second decryption operation to decode the PIN data, wherein said second decryption operation is different from the first decryption operation.

7. (original) The method of decoding encrypted transaction data of claim 6, wherein: said first decryption operation uses a symmetrical decryption process; and said second decryption operation uses an asymmetrical decryption process.

8. (original) The method of decoding encrypted transaction data of claim 6, further comprising the steps:

a2 calculating a digest by applying a one-way mathematical process to the non-PIN data; and

comparing the calculated digest to a received digest formed with the same one-way mathematical process and appended to the PIN data blocks for verifying the non-PIN data.

9. (currently amended) A method for encoding account related data comprising the steps:

analyzing the account related data to identify PIN-related data blocks input by a user and non-PIN data blocks;

performing a first encryption operation only on said PIN-related data blocks; and

performing a second encryption operation on at least said non-PIN data blocks.

10. (original) The method for encoding account related data of claim 9, wherein: said first encryption operation uses an asymmetrical encryption process; and said second encryption operation uses a symmetrical encryption process.

11. (original) The method for encoding account related data of claim 10, wherein said symmetrical encryption process uses a secret encryption key and wherein said method includes the further step of performing a third encryption operation on said secret encryption key.

12. (original) The method for encoding account related data of claim 10, wherein said second encryption operation is performed on both the PIN and non-PIN data, such that the encrypted PIN data resides within an encrypted envelope generated by the second encryption operation.

a2

13. (original) The method of encoding account related data of claim 9, further comprising the steps of:

calculating a digest by applying a one-way mathematical process to the non-PIN data; and

appending the digest to the PIN data blocks to allow for future verification of the non-PIN data.

14. (original) The method of encoding account data of claim 9, wherein the account data is associated with a payment instrument selected from the group including a credit card, a debit card and a "smart" card.

15. (currently amended) A method of transporting PIN data input by a user and non-PIN data in a secure electronic transfer, comprising the steps:

encrypting only the PIN data using a first encryption process,

encrypting at least the non-PIN data using a second encryption process;

transmitting the encrypted PIN and non-PIN data to an authentication requestor, said authentication requestor having means to decrypt only the non-PIN data;

transmitting the encrypted PIN data to an authorizing agent for verification;

decrypting and verifying the PIN data by the authorizing agent; and

transmitting a notification, from the authorizing agent to the authentication requestor, of a verification status of the PIN data.

a2

16. (original) The method of transporting PIN and non-PIN data of claim 15, wherein said second encryption process is different from the first encryption process;

17. (original) The method of transporting PIN and non-PIN data of claim 16, wherein: said first encryption process is an asymmetrical encryption process; and said second encryption process is a symmetrical encryption process.

18. (original) The method of transporting PIN and non-PIN data of claim 17, wherein the asymmetrical encryption process is performed using a public key provided to an account holder by the authorizing agent and wherein said decrypting performed by the authorizing agent is performed using a private key associated with the public key.

19. (original) The method of transporting PIN and non-PIN data of claim 18, wherein said symmetrical encryption process uses a secret encryption key and wherein said method includes the further step of performing a third encryption operation on said secret encryption key.

20. (original) The method of transporting PIN and non-PIN data of claim 16, further comprising the steps of:

prior to transmitting the encrypted PIN and non-PIN data, calculating a first digest by applying a one-way mathematical process to the non-PIN data and appending the digest to the PIN data blocks; and

after transmitting the encrypted PIN and non-PIN data, calculating a second digest by applying the same one-way mathematical process to the non-PIN data and comparing the first digest and second digest to verify the non-PIN data.

21. (currently amended) A terminal for encoding transaction data including account PIN data input by a user as well as non-PIN data, comprising:

means for performing a first encryption operation only on the PIN data; and

means for performing a second encryption operation on at least the non-PIN data, such that the PIN data is cryptographically isolated from the non-PIN data.

22. (original) The terminal for encoding transaction data of claim 21, wherein: said first encryption means uses an asymmetrical encryption process; and said second encryption means uses a symmetrical encryption process.

23. (original) The terminal for encoding transaction data of claim 21, further comprising a card reader for acquiring at least a portion of the transaction data from a payment instrument.

24. (currently amended) A system for decoding encrypted transaction data including account PIN data input by a user as well as non-PIN data, comprising:

a2

means for performing a first decryption operation to decode the non-PIN data; and

means for performing a second decryption operation to decode the PIN data, wherein said second decryption operation is different from the first decryption operation.

25. (original) The system as defined by claim 24, wherein: said first decryption means uses a symmetrical decryption process; and said second decryption means uses an asymmetrical decryption process.

26. (currently amended) A system for encoding and transporting PIN data input by a user and non-PIN data comprising:

first means for encrypting only the PIN data using a first encryption process;

second means for encrypting at least the non-PIN data using a second encryption process;

means for transmitting the encrypted PIN and non-PIN data to an authentication requestor, said authentication requestor having means to decrypt only the non-PIN data;

means for transmitting the encrypted PIN data to an authorizing agent for verification;

means for decrypting and verifying the PIN data by the authorizing agent; and

means for notifying the authentication requestor of a verification status of the PIN data.

27. (original) The system for encoding and transporting PIN and non-PIN data of claim 26, wherein said second encryption process is different from the first encryption process

28. (original) The system for encoding and transporting PIN and non-PIN data of claim 27, wherein:

said first encryption means employs an asymmetrical encryption process; and

said second encryption means employs a symmetrical encryption process.

29. (original) The system for encoding and transporting PIN and non-PIN data of claim 27, wherein the first encryption means uses a public key provided to an account holder by the authorizing agent and wherein said decrypting means uses a private key associated with the public key.

30. (original) The system for encoding and transporting PIN and non-PIN data of claim 26, further comprising:

means for calculating a first digest by applying a one-way mathematical process to the non-PIN data and appending the digest to the PIN data blocks prior to transmitting the encrypted PIN and non-PIN data; and

means for calculating a second digest by applying the same one-way mathematical process to the non-PIN data and comparing the first digest and second digest after transmitting the encrypted PIN and non-PIN data, to verify the non-PIN data.

a2

31. (original) The system for encoding and transporting PIN and non-PIN data of claim 24, further comprising a card reader for acquiring at least a portion of the PIN and non-PIN data from a payment instrument.